UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/652,899	08/31/2000	Fred Alan Bishop	10655.8000	3558

66283 7590 02/09/2007 AMERICAN EXPRESS COMPANY C/O MCDERMOTT WILL & EMERY LLP 227 WEST MONROE STREET, SUITE 4400 CHICAGO, IL 60606-5096	**EXAMINER** WORJLOH, JALATEE

ART UNIT	PAPER NUMBER
3621	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/09/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

	Application No.	Applicant(s)
Office Action Summary	09/652,899	BISHOP ET AL.
	Examiner	Art Unit
	Jalatee Worjloh	3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *January 3, 2007.*

2a)☐ This action is **FINAL.**   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle,* 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4, 43-46 and 90-103* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4, 43-46 and 90-103* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____.

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1.   A request for continued examination under 37 CFR 1.114, including the fee set forth in

37 CFR 1.17(e), was filed in this application after final rejection. Since this application is

eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e)

has been timely paid, the finality of the previous Office action has been withdrawn pursuant to

37 CFR 1.114. Applicant's submission filed on January 3, 2007 has been entered.

Claim Rejections - 35 USC § 103

2.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

3.   Claims 1-3, 43-45 and 90 are rejected under 35 U.S.C. 103(a) as being unpatentable over

U.S. Patent No. 6263446 to Kausik et al. in view of US Patent No. 6327578 to Linehan.

Referring to claim 1, Kausik et al. disclose receiving at a first server (i.e. credential

server), a transaction request from a user for a transaction at a merchant server (see claim 30(a) –

receiving from a requestor, over a network a request for a predetermined authentication

credential), issuing a challenge to the user, wherein said challenge is passed to an intelligent

token for processing said challenge, (see claim 30 (b) – transmitting, to said requestor, a

challenge; claim 34 – said transmitting is to a digital wallet of said requestor; col. 4, lines 35-46

– the wallet could be installed onto the hard drive or other physical memory of the computer ...

the invention could also be used in conjunction with a physical token), wherein said intelligent

token (i.e. physical token) generates a response to said challenge, receiving said response from

the user based upon said challenge (see claim 30 (c) – receiving an answer to said challenge),

processing said response to verify the intelligent token (see claim 30 (d) – determining that said

answer satisfies said challenge ; claim 34 and col. 4-lines 35-46 – physical token), providing at

least a portion of said assembled credentials to said user (see claim 30 (e) transmitting said

authentication credential for said requestor and claim 32 – said credential is a private key),

receiving, at a second server (i.e. access control server), a second request from said user, said

second request including said portion of said assembled credentials provided to said user, and

validating at said second server, said portion of said assembled credentials provided to said user

with said key of said assembled credentials to provide access to a transaction service (see col. 3,

lines 43-49 & 61-63). As for assembling credentials for the transaction at said first server, said

credentials comprising at least one key, this is an inherent step. Notice, Kausik et al. the

authentication credential is in existence at said server prior to the request (see claim 30, (a) (i)),

which implies that the credential has been created. Claim 32 discloses a credential that is a

private key. Kausik et al. do not expressly disclose issuing a challenge to a third server and

forwarding the challenge from said third server to the user, receiving said response at said third

server and processing said response at said third server. Linehan discloses issuing a challenge to

a third server (i.e. consumer's computer) and forwarding the challenge from said third server to

the user (i.e. smart card reader, which passes it on to the smart card), receiving said response at

said third server and processing said response at said third server (see col. 7, lines 25-37). At the

time the invention was made, it would have been obvious to a person of ordinary skill in the art

to modify the method disclose by Kausik et al. to include the steps of issuing a challenge to a

third server and forwarding the challenge from said third server to the user, receiving said

response at said third server and processing said response at said third server. One of ordinary

skill in the art would have been motivated to do this because it provides an additional level of

security and protection for all entities involved in the transaction (see col. 7, lines 3-5 & 33-38).

Referring to claims 2 and 44, Kausik et al. disclose the transaction is an electronic

purchase transaction (see col. 3, lines 22-24).

Referring to claims 3 and 45, Kausik et al. disclose the electronic purchase transaction is

conducted using a digital wallet (see claim 34).

Referring to claim 43, Kausik et al. disclose receiving, at a first server (i.e.

credential server), a transaction request from a user for a transaction at a merchant server (see

claim 30(a) – receiving from a requestor, over a network a request for a predetermined

authentication credential), issuing a challenge to the user, wherein said challenge is passed to an

intelligent token (i.e. physical token) for processing said challenge, (see claim 30 (b) –

transmitting, to said requestor, a challenge; claim 34 – said transmitting is to a digital wallet of

said requestor; col. 4, lines 35-46 – the wallet could be installed onto the hard drive or other

physical memory of the computer … the invention could also be used in conjunction with a

physical token), wherein said intelligent token generates a response to said challenge, receiving

said response from the user based upon said challenge (see claim 30 (c) – receiving an answer to

said challenge), processing said response to verify the intelligent token (see claim 30 (d) –

determining that said answer satisfies said challenge ; claim 34 and col. 4-lines 35-46 – physical

token), providing at least a portion of said assembled credentials to said user (see claim 30 (e)

transmitting said authentication credential for said requestor and claim 32 – said credential is a private key), receiving, at a second server (i.e. access control server), a second request from said user, said second request including said portion of said assembled credentials provided to said user, and validating at said second server, said portion of said assembled credentials provided to said user with said key of said assembled credentials to provide access to a transaction service (see col. 3, lines 43-49 & 61-63). As for assembling credentials for the transaction at said first server, said credentials comprising at least one key, this is an inherent step. Notice, Kausik et al. the authentication credential is in existence at said server prior to the request (see claim 30, (a) (i)), which implies that the credential has been created. Claim 32 discloses a credential that is a private key. Kausik et al. do not expressly disclose issuing a challenge to a third server and forwarding the challenge from said third server to the user, receiving said response at said third server and processing said response at said third server. Linehan discloses issuing a challenge to a third server (i.e. consumer's computer) and forwarding the challenge from said third server to the user (i.e. smart card reader, which passes it on to the smart card), receiving said response at said third server and processing said response at said third server (see col. 7, lines 25-37). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the method disclose by Kausik et al. to include the steps of issuing a challenge to a third server and forwarding the challenge from said third server to the user, receiving said response at said third server and processing said response at said third server. One of ordinary skill in the art would have been motivated to do this because it provides an additional level of security and protection for all entities involved in the transaction (see col. 7, lines 3-5 & 33-38).

Referring to claim 90, Kausik et al. disclose receiving at a first server (i.e. credential

server), a transaction request from a user for a transaction at a merchant server (see claim 30(a) –

receiving from a requestor, over a network a request for a predetermined authentication

credential), issuing a challenge to the user, wherein said challenge is passed to an intelligent

token (i.e. physical token) for processing said challenge, (see claim 30 (b) – transmitting, to said

requestor, a challenge; claim 34 – said transmitting is to a digital wallet of said requestor; col. 4,

lines 35-46 – the wallet could be installed onto the hard drive or other physical memory of the

computer ... the invention could also be used in conjunction with a physical token), wherein said

intelligent token generates a response to said challenge, receiving a response from the user based

upon said challenge (see claim 30 (c) – receiving an answer to said challenge), processing said

response to verify the intelligent token (see claim 30 (d) – determining that said answer satisfies

said challenge ; claim 34 and col. 4-lines 35-46 – physical token), providing at least a portion of

said assembled credentials to said user (see claim 30 (e) transmitting said authentication

credential for said requestor and claim 32 – said credential is a private key), receiving, at a

second server (i.e. access control server), a second request from said user indicating readiness to ·

complete the transaction, said second request including said portion of said assembled

credentials provided to said user, and validating at said second server, said portion of said

assembled credentials provided to said user with said key of said assembled credentials to

thereby permit processing and completion of said transaction (see col. 3, lines 43-49 & 61-63).

As for assembling credentials for the transaction at said first server, said credentials comprising

at least one key, this is an inherent step. Notice, Kausik et al. the authentication credential is in

existence at said server prior to the request (see claim 30, (a) (i)), which implies that the

credential has been created. Claim 32 discloses a credential that is a private key. Kausik et al. do

not expressly disclose issuing a challenge to a third server and forwarding the challenge from

said third server to the user, receiving said response at said third server and processing said

response at said third server. Linehan discloses issuing a challenge to a third server (i.e.

consumer's computer) and forwarding the challenge from said third server to the user (i.e. smart

card reader, which passes it on to the smart card), receiving said response at said third server and

processing said response at said third server (see col. 7, lines 25-37). At the time the invention

was made, it would have been obvious to a person of ordinary skill in the art to modify the

method disclose by Kausik et al. to include the steps of issuing a challenge to a third server and

forwarding the challenge from said third server to the user, receiving said response at said third

server and processing said response at said third server. One of ordinary skill in the art would

have been motivated to do this because it provides an additional level of security and protection

for all entities involved in the transaction (see col. 7, lines 3-5 & 33-38).

4.   Claims 4, 46 and 91-103 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Kausik et al. and Linehan as applied to claims 1 and 90 above, and further in view of U.S. Patent

No. 6873974 to Schutzer.

        Referring to claims 4, 96 and 101, Kausik et al. disclose an intelligent token (see claim 1

above – "physical token"). Kausik et al. do not expressly disclose the intelligent token is a smart

card. Schutzer discloses the intelligent token is a smart card (see col. 9, lines 16-24). At the

time the invention was made, it would have been obvious to a person of ordinary skill in the art

to modify the method disclose by Kausik et al. to include an intelligent token that is a smart card.

One of ordinary skill in the art would have been motivated to do this because smart cards are more secure than software wallets and they can be conveniently carried as the user roams (see Kausik et al. col. 1, lines 56-58).

Referring to claim 46, Kausik et al. disclose a user conducts a transaction via a wallet (see claim 43 above). Kausik et al. do not expressly disclose the user conducts the transaction via a smart card. Schutzer discloses the user conducts the transaction via a smart card (see col. 9, liens 16-24). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the method disclose by Kausik et al. to include the step wherein the user conducts the transaction via a smart card. One of ordinary skill in the art would have been motivated to do this because smart cards are more secure than software wallets and they can be conveniently carried as the user roams (see Kausik et al. col. 1, liens 56-58).

Referring to claim 91, Kausik et al. disclose a user, and second server (see claim 90 above). Kausik et al. do not expressly disclose accessing required information associated with said user from said second server, populating one or more corresponding user purchase forms at said second server with said required information and said second server providing said populated user purchase forms and an authorization response message to a merchant for processing and completion of said transaction. Schutzer discloses accessing required information associated with said user from said second server, populating one or more corresponding user purchase forms at said second server with said required information and said second server providing said populated user purchase forms and an authorization response message to a merchant for processing and completion of said transaction (see col. 2, lines 15-27). At the time the invention was made, it would have been obvious to a person of ordinary skill in

the art to modify the method disclose by Kausik et al. to include the steps of accessing required

information associated with said user from said second server, populating one or more

corresponding user purchase forms at said second server with said required information and said

second server providing said populated user purchase forms and an authorization response

message to a merchant for processing and completion of said transaction. One of ordinary skill

in the art would have been motivated to do this because it provides an electronic system that

allows users to easily interact with merchants.

Referring to claims 92, 93, 100 and 102, Kausik et al. disclose the transaction is an

electronic purchase transaction and the transaction is a web-based purchase transaction (see col.

3, lines 22-24).

Referring to claims 94 and 95, Kausik et al. disclose the electronic purchase transaction is

conducted using a digital wallet (see claim 34).

Referring to claims 97 and 103, Kausik et al. disclose an electronic transaction system

(see claim 91 above). Kausik et al. do not expressly disclose said required information includes

user name, user address, shipping address, card number and payment amount. Schutzer disclose

said required information includes user name, user address, shipping address, card number and

payment amount (see abstract). At the time the invention was made, it would have been obvious

to a person of ordinary skill in the art to modify the method disclose by Kausik to include said

required information includes user name, user address, shipping address, card number and

payment amount. One of ordinary skill in the art would have been motivated to do this because

it provides an electronic system that allows users to easily interact with merchants.

Referring to claim 98, Kausik et al. disclose receiving at a first server (i.e. credential

server), a transaction request from a user for a transaction at a merchant server (see claim 30(a) –

receiving from a requestor, over a network a request for a predetermined authentication

credential), issuing a challenge to the user, wherein said challenge is passed to an intelligent

token (i.e. physical token) for processing said challenge, (see claim 30 (b) – transmitting, to said

requestor, a challenge; claim 34 – said transmitting is to a digital wallet of said requestor; col. 4,

lines 35-46 – the wallet could be installed onto the hard drive or other physical memory of the

computer ... the invention could also be used in conjunction with a physical token), wherein said

intelligent token generates a response to said challenge, receiving a response from the user based

upon said challenge (see claim 30 (c) – receiving an answer to said challenge), processing said

response to verify the intelligent token (see claim 30 (d) – determining that said answer satisfies

said challenge ; claim 34 and col. 4-lines 35-46 – physical token), providing at least a portion of

said assembled credentials to said user (see claim 30 (e) transmitting said authentication

credential for said requestor and claim 32 – said credential is a private key), receiving, at a

second server (i.e. access control server), a second request from said user, said second request

including said portion of said assembled credentials provided to said user, and validating at said

second server, said portion of said assembled credentials provided to said user with said key of

said assembled credentials to thereby permit processing and completion of said transaction (see

col. 3, lines 43-49 & 61-63). As for assembling credentials for the transaction at said first server,

said credentials comprising at least one key, this is an inherent step. Notice, Kausik et al. the

authentication credential is in existence at said server prior to the request (see claim 30, (a) (i)),

which implies that the credential has been created. Claim 32 discloses a credential that is a

private key. Kausik et al. do not expressly disclose accessing required information associated

with said user from said second server, populating, at said second server, one or more

corresponding user purchase forms with said required information and said second server

providing said populated user purchase forms and an authorization response message to a

merchant for processing and completing said purchase transaction. Schutzer discloses accessing

required information associated with said user from said second server, populating one or more

corresponding user purchase forms at said second server with said required information and said

second server providing said populated user purchase forms and an authorization response

message to a merchant for processing and completion of said transaction (see col. 2, lines 15-27).

At the time the invention was made, it would have been obvious to a person of ordinary skill in

the art to modify the method disclose by Kausik et al. to include the steps of accessing required

information associated with said user from said second server, populating one or more

corresponding user purchase forms at said second server with said required information and said

second server providing said populated user purchase forms and an authorization response

message to a merchant for processing and completion of said transaction. One of ordinary skill

in the art would have been motivated to do this because it provides an electronic system that

allows users to easily interact with merchants.

Referring to claim 99, Kausik et al. disclose receiving said challenge at said intelligent

token (see claim 30 (b) and claim 34 – transmitting, to said requestor, a challenge…said

transmitting is to a digital wallet of a requestor), receiving said personal identifier (i.e. PIN) from

said user, said instrument validating said personal identifier sand unlocking said instrument (see

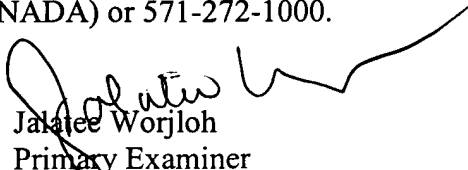col. 5, lines 10- 24, the user enters a PIN to unlock the wallet…the PIN is compared with a

stored hash value...if the two hash values agree, the PIN is passed to decryption module...the decrypted private key is released for use), said intelligent token transmitting said response to said first server (see claim 30 (c)). As for the step of said intelligent token prompting said user for a personal identifier this is an inherent step. That is, before the user enters the PIN, he must have previously been prompted for such entry.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jalatee Worjloh whose telephone number is (571) 272-6714. The examiner can normally be reached on Mondays-Thursdays 8:30 - 7:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Fischer can be reached on (571) 272-6779. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300 for Regular/After Final Actions and 571-273-6714 for Non-Official/Draft.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jalatee Worjloh
Primary Examiner
Art Unit 3621

January 29, 2007